

# CARTAN SUBALGEBRAS IN GENERAL AND SPECIAL LINEAR ALGEBRAS

KYOUNG-TARK KIM

**ABSTRACT.** In this paper we study Cartan subalgebras in general and special linear algebras over a field of positive characteristic. We determine the conjugacy classes of Cartan subalgebras under the general linear groups, and count the explicit number of all Cartan subalgebras from its conjugacy when the base field is an arbitrary finite field.

## 1. INTRODUCTION

Let  $\mathbb{K}$  be a field of positive characteristic  $p$ . By the *general linear algebra*  $\mathfrak{gl}(n, \mathbb{K})$  we mean the vector space of all  $n \times n$  matrices over  $\mathbb{K}$  together with a unary operation  $X \mapsto X^p$ , called the *p-map*, and a binary operation  $(X, Y) \mapsto [X, Y] = XY - YX$ , called the *commutator* or the *Lie bracket* where  $X$  and  $Y$  are in  $\mathfrak{gl}(n, \mathbb{K})$ . The *special linear algebra*  $\mathfrak{sl}(n, \mathbb{K})$  is the subspace of all trace zero matrices in  $\mathfrak{gl}(n, \mathbb{K})$  together with the inherited operations. (It is well-known and easy to see that  $\mathfrak{sl}(n, \mathbb{K})$  is closed under the *p-map* and the commutator.)

A *torus*  $\mathfrak{T}$  is defined as a subspace of  $\mathfrak{gl}(n, \mathbb{K})$  satisfying

- (T1)  $\mathfrak{T}$  is closed under the *p-map*;
- (T2)  $[X, Y] = 0$  for all  $X, Y \in \mathfrak{T}$ ;
- (T3) each matrix in  $\mathfrak{T}$  is *absolutely semisimple*, i.e., diagonalizable over an algebraic closure  $\mathbb{k}$  of  $\mathbb{K}$ .

Let  $\mathfrak{D}$  and  $\mathfrak{D}_0$  be respectively the subsets of all diagonal matrices in  $\mathfrak{gl}(n, \mathbb{K})$  and  $\mathfrak{sl}(n, \mathbb{K})$ . Clearly,  $\mathfrak{D}$  and  $\mathfrak{D}_0$  are tori with  $\dim \mathfrak{D} = n$  and  $\dim \mathfrak{D}_0 = n - 1$ . They are maximal by the following basic observation:

**Proposition 1.1.** *Let  $\mathfrak{T}$  be a torus. Then,  $\mathfrak{T}$  is maximal in  $\mathfrak{gl}(n, \mathbb{K})$  (in  $\mathfrak{sl}(n, \mathbb{K})$ , respectively) if and only if  $\dim \mathfrak{T}$  is equal to  $n$  (resp.  $n - 1$ ).*

*Proof.* Since all matrices in  $\mathfrak{T}$  commute there is  $U \in \mathrm{GL}(n, \mathbb{k})$  such that  $U^{-1}\overline{\mathfrak{T}}U \subseteq \overline{\mathfrak{D}}$  where, for any  $\mathbb{K}$ -vector space  $\mathfrak{V}$ ,  $\overline{\mathfrak{V}} := \mathbb{k} \otimes_{\mathbb{K}} \mathfrak{V}$  denotes the usual scalar extension. Since  $\dim_{\mathbb{k}} \overline{\mathfrak{D}} = \dim_{\mathbb{K}} \mathfrak{D} = n$  and  $\dim_{\mathbb{k}} U^{-1}\overline{\mathfrak{T}}U = \dim_{\mathbb{K}} \mathfrak{T}$  we have  $\dim_{\mathbb{K}} \mathfrak{T} \leq n$ . So if  $\dim_{\mathbb{K}} \mathfrak{T} = n$  then  $\mathfrak{T}$  is maximal in  $\mathfrak{gl}(n, \mathbb{K})$ . Conversely suppose that  $\mathfrak{T}$  is maximal in  $\mathfrak{gl}(n, \mathbb{K})$ . Since  $\overline{\mathfrak{T}}$  (hence  $U^{-1}\overline{\mathfrak{T}}U$ ) is a maximal torus in  $\mathfrak{gl}(n, \mathbb{k})$  by [3, Theorem 2.15, p. 73], we have  $\dim_{\mathbb{K}} \mathfrak{T} = n$ . The proof in  $\mathfrak{sl}(n, \mathbb{K})$  is similar.  $\square$

In a Lie algebra  $\mathfrak{g}$  of arbitrary characteristic one can define a *Cartan subalgebra* (abbreviated, *CSA*)  $\mathfrak{h}$  as a Lie subalgebra of  $\mathfrak{g}$  satisfying

- (C1)  $\mathfrak{H}$  is a nilpotent Lie algebra;
- (C2) the normalizer of  $\mathfrak{H}$  in  $\mathfrak{g}$  is  $\mathfrak{H}$  itself, i.e.,  $\mathfrak{H}$  is self-normalizing.

Traditionally the role of CSAs is central in the theory of finite dimensional Lie algebras of characteristic zero: The definition of a CSA gives the *Fitting-Zassenhaus* decomposition of a Lie algebra. In the case of characteristic zero, the existence of a CSA was proved by showing that a CSA is the centralizer of a *regular* element, namely, a minimal *Engel* subalgebra. Moreover, when the base field is algebraically closed, the well-known conjugacy theorem for CSAs assures the ‘uniqueness’.

In this paper we focus on CSAs in general and special linear algebras (which are probably the most naive to understand) over a field of positive characteristic, and consider the structure and the conjugacy problems about them. In particular, when the ground field is finite, we concentrate on counting problem for CSAs.

In fact the algebraic structures like  $\mathfrak{gl}(n, \mathbb{K})$  or  $\mathfrak{sl}(n, \mathbb{K})$  have a given name - a *restricted Lie algebras* or a *Lie  $p$ -algebras* - initially introduced by N. Jacobson. In a restricted Lie algebra there is a fundamental connection between CSAs and maximal tori:

**Theorem 1.2.** [3] *Let  $\mathfrak{g}$  be a restricted Lie algebra. Then,  $\mathfrak{H}$  is a CSA of  $\mathfrak{g}$  if and only if  $\mathfrak{H}$  is the centralizer of a maximal torus in  $\mathfrak{g}$ .*

From the later sections of this paper we shall obtain the followings:

**Proposition 1.3.** *Every maximal torus in  $\mathfrak{gl}(n, \mathbb{K})$  is self-centralizing.*

*Proof.* It follows from Propositions 1.1, 2.2 and Lemma 2.6.  $\square$

**Proposition 1.4.** *If  $p = 2$  then  $\mathfrak{sl}(2, \mathbb{K})$  is nilpotent. If  $p > 2$  or  $n > 2$  then every maximal torus in  $\mathfrak{sl}(n, \mathbb{K})$  is self-centralizing.*

*Proof.* If  $\text{char } \mathbb{K} = 2$  then a basis for  $\mathfrak{sl}(2, \mathbb{K})$  is  $\{(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}), (\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}), (\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix})\}$ . Since  $[\mathfrak{sl}(2, \mathbb{K}), \mathfrak{sl}(2, \mathbb{K})] = \mathbb{K}(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})$  and  $[\mathfrak{sl}(2, \mathbb{K}), \mathbb{K}(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})] = 0$ ,  $\mathfrak{sl}(2, \mathbb{K})$  is nilpotent. The second assertion follows from Corollary 4.5.  $\square$

Therefore the maximal tori in  $\mathfrak{gl}(n, \mathbb{K})$  or  $\mathfrak{sl}(n, \mathbb{K})$  are precisely the CSAs by Theorem 1.2 and Propositions 1.3, 1.4 unless  $p = n = 2$ , in which case, we know that  $\mathfrak{sl}(2, \mathbb{K})$  is itself a CSA.

In section 2 we prepare and study basic structures of maximal tori in  $\mathfrak{gl}(n, \mathbb{K})$ . In section 3 we finally gain the number of all maximal tori in  $\mathfrak{gl}(n, \mathbb{K})$  when  $\mathbb{K}$  is an arbitrary finite field. This result follows from a consideration about the conjugacy classes under  $\text{GL}(n, \mathbb{K})$ . In section 4 we consider the case in  $\mathfrak{sl}(n, \mathbb{K})$ . In particular we also obtain the number of all maximal tori in  $\mathfrak{sl}(n, \mathbb{K})$  when  $\mathbb{K}$  is a finite field.

## 2. BASIC STUDY IN MAXIMAL TORI IN $\mathfrak{gl}(n, \mathbb{K})$

In this section we denote by  $\mathfrak{M}$  a torus which is *maximal* in  $\mathfrak{gl}(n, \mathbb{K})$ .

**Proposition 2.1.** *The following hold for a maximal torus in  $\mathfrak{gl}(n, \mathbb{K})$ .*

- (i)  $\mathfrak{M}$  is closed under the matrix product;
- (ii)  $I_n \in \mathfrak{M}$  where  $I_n$  is the  $n \times n$  identity matrix.

*Proof.* (i) Let  $X$  and  $Y$  in  $\mathfrak{M}$ . Since  $XY = YX$ ,  $X$  and  $Y$  are simultaneously diagonalizable over  $\mathbb{k}$ . So  $XY$  is absolutely semisimple. Since  $XY$  commutes with all matrices in  $\mathfrak{M}$  the maximality of  $\mathfrak{M}$  implies  $\mathfrak{M} + \sum_{i=0}^{\infty} \mathbb{K}(XY)^{p^i} = \mathfrak{M}$ , i.e.,  $XY \in \mathfrak{M}$ . (ii) Since  $I_n$  is diagonal and commutes with all matrices in  $\mathfrak{M}$  the maximality yields  $I_n \in \mathfrak{M}$ .  $\square$

**Proposition 2.2.**  $\mathfrak{M}$  is a semisimple commutative algebra over  $\mathbb{K}$ .

*Proof.* By Proposition 2.1,  $\mathfrak{M}$  is a commutative associative  $\mathbb{K}$ -algebra. Since  $\mathfrak{M}$  has no nonzero nilpotent matrix  $\mathfrak{M}$  is semisimple.  $\square$

**Corollary 2.3.** We have  $\mathfrak{M} \cong \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_t$  as associative  $\mathbb{K}$ -algebras where  $\mathbb{F}_i$  is a separable extension field of  $\mathbb{K}$  for each  $i \in \{1, \dots, t\}$ .

*Proof.* By Proposition 2.2 and the Wedderburn structure theorem we know  $\mathfrak{M} \cong \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_t$  for some extension fields  $\mathbb{F}_1, \dots, \mathbb{F}_t$  of  $\mathbb{K}$ . Since every element of  $\mathfrak{M}$  is diagonalizable the minimal polynomial over  $\mathbb{K}$  of an element of  $\mathbb{F}_i$  must be separable, i.e.,  $\mathbb{F}_i$  is separable over  $\mathbb{K}$ .  $\square$

Let  $\varphi : \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_t \rightarrow \mathfrak{M}$  be an isomorphism. Put  $E_i := \varphi(1_{\mathbb{F}_i})$  for each  $i \in \{1, \dots, t\}$ . Then  $E_1, \dots, E_t$  are orthogonal primitive idempotents with  $I_n = \sum E_i$ . Since these are uniquely determined by  $\mathfrak{M}$  so are  $n_i := \dim \mathfrak{M}E_i = \dim_{\mathbb{K}} \mathbb{F}_i$ . We may assume that  $n_1 \geq \cdots \geq n_t$ .

**Definition 2.4.** The sequence  $(n_1, \dots, n_t)$  is called the *type* of  $\mathfrak{M}$ .

- (i)  $\mathfrak{M}$  is called *division* if  $\mathfrak{M}$  has type  $(n)$ .
- (ii)  $\mathfrak{M}$  is called *split* if  $\mathfrak{M}$  has type  $(1, \dots, 1)$ ;

**Definition 2.5.** Let  $A_1$  and  $A_2$  be associative  $\mathbb{K}$ -algebras. Let  $M_1$  be an  $A_1$ -module and  $M_2$  an  $A_2$ -module. We say that  $M_1$  is *equivalent* to  $M_2$  if there exist an isomorphism  $f : A_1 \rightarrow A_2$  and a  $\mathbb{K}$ -linear bijection  $g : M_1 \rightarrow M_2$  such that  $g(am) = f(a)g(m)$  for all  $a \in A_1$  and  $m \in M_1$ .

Evidently, the regular modules for  $\mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_t$  and  $\mathfrak{M}$  are equivalent via the map  $\varphi$ . Moreover we know the following fundamental fact:

**Lemma 2.6.** Let  $\mathfrak{A} \subseteq \text{Mat}(n, \mathbb{K})$  be a semisimple commutative algebra over  $\mathbb{K}$  with  $I_n$ . Then there is an  $\mathfrak{A}$ -module monomorphism  $\mathfrak{A} \hookrightarrow \mathbb{K}^n$ .

*Proof.* Since  $\mathfrak{A}$  is semisimple,  $\mathfrak{A} = \mathfrak{I}_1 \oplus \cdots \oplus \mathfrak{I}_t$  where  $\mathfrak{I}_i$ 's are irreducible  $\mathfrak{A}$ -modules, i.e., minimal left ideals of  $\mathfrak{A}$ . Since  $\mathfrak{A}$  is commutative,  $\mathfrak{I}_i$ 's are indeed two-sided ideals of  $\mathfrak{A}$ . Therefore if  $I_n = A_1 + \cdots + A_t$  for some  $A_i \in \mathfrak{I}_i$  then  $A_1, \dots, A_t$  are orthogonal primitive idempotents in  $\mathfrak{A}$ . Since  $A_i \neq 0$  we can choose  $v_i \in \mathbb{K}^n$  such that  $A_i v_i \neq 0$ . If we define  $\psi_i : \mathfrak{I}_i \rightarrow A_i \mathbb{K}^n$  to be an  $\mathfrak{A}$ -module homomorphism generated by  $A_i \mapsto A_i v_i$  then  $\psi_i$  is injective whence so is  $\psi_1 \oplus \cdots \oplus \psi_t : \mathfrak{A} \rightarrow \mathbb{K}^n$ .  $\square$

**Corollary 2.7.** The regular module for  $\mathfrak{M}$  is isomorphic to the standard module  $\mathbb{K}^n$  for  $\mathfrak{M}$  (defined from the inclusion  $\mathfrak{M} \subseteq \text{Mat}(n, \mathbb{K})$ ).

*Proof.* Since  $\dim \mathfrak{M} = \dim \mathbb{K}^n$  we are done by Lemma 2.6.  $\square$

The regular module for  $\mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_t$  gives rise to an equivalent module  $\mathbb{K}^n$ : If  $\{\xi_1^{(k)}, \dots, \xi_{n_k}^{(k)}\}$  is a  $\mathbb{K}$ -basis of  $\mathbb{F}_k$  for each  $k \in \{1, \dots, t\}$  then we define a (faithful) regular representation  $\rho_k : \mathbb{F}_k \rightarrow \text{Mat}(n_k, \mathbb{K})$  by  $\rho_k(\eta) := (\alpha_{i,j}(\eta))$  where  $\eta \xi_j^{(k)} = \sum_{i=1}^{n_k} \alpha_{i,j}(\eta) \xi_i^{(k)}$  for  $j \in \{1, \dots, n_k\}$ . Since  $\rho_1(\mathbb{F}_1) \oplus \cdots \oplus \rho_t(\mathbb{F}_t)$  can be regarded as a direct sum in  $\text{Mat}(n, \mathbb{K})$  we obtain an equivalent module  $\mathbb{K}^n$  for  $\rho_1(\mathbb{F}_1) \oplus \cdots \oplus \rho_t(\mathbb{F}_t)$  via the correspondence  $\{\xi_j^{(k)} \mid k \in \{1, \dots, t\}, j \in \{1, \dots, n_k\}\} \leftrightarrow \{e_1, \dots, e_n\}$  where  $e_i \in \mathbb{K}^n$  is the standard unit vector in  $\mathbb{K}^n$  for each  $i \in \{1, \dots, n\}$ .

**Proposition 2.8.** *We have  $U^{-1}\mathfrak{M}U = \rho_1(\mathbb{F}_1) \oplus \cdots \oplus \rho_t(\mathbb{F}_t)$  for some  $U \in \text{GL}(n, \mathbb{K})$  and regular representations  $\rho_i : \mathbb{F}_i \rightarrow \text{Mat}(n_i, \mathbb{K})$ .*

*Proof.* From Corollary 2.7 and the preceding argument we conclude that the modules  $\mathbb{K}^n$  for  $\mathfrak{M}$  and  $\rho_1(\mathbb{F}_1) \oplus \cdots \oplus \rho_t(\mathbb{F}_t)$  are equivalent.  $\square$

### 3. MAXIMAL TORI IN $\mathfrak{gl}(n, \mathbb{K})$ WHEN $\mathbb{K}$ IS FINITE

Our goal of this section is to obtain the number of all maximal tori (or Cartan subalgebras) in  $\mathfrak{gl}(n, \mathbb{K})$  when  $\mathbb{K}$  is a finite field with  $\text{char } \mathbb{K} = p$ .

Throughout this section we put  $q := p^\ell$  and assume  $\mathbb{K} = \mathbb{F}_q$ , that is, a finite field with  $p^\ell$  elements. We use the symbol  $\mathfrak{M}$  as a maximal torus in  $\mathfrak{gl}(n, \mathbb{K})$ . Also we shall frequently see the following notations:

- (i)  $\text{Cl}(\mathfrak{M}) := \{U^{-1}\mathfrak{M}U \mid U \in \text{GL}(n, q)\};$
- (ii)  $\text{N}(\mathfrak{M}) := \{U \in \text{GL}(n, q) \mid U^{-1}\mathfrak{M}U = \mathfrak{M}\}.$

**Proposition 3.1.** *The type of  $\mathfrak{M}$  determines the conjugacy class  $\text{Cl}(\mathfrak{M})$ . The number of all conjugacy classes is the partition number of  $n$ .*

*Proof.* Any two extension fields of a finite field  $\mathbb{K}$  are isomorphic if the extension degrees coincide. So the first assertion is a consequence of Proposition 2.8. The second assertion follows from the first.  $\square$

**Lemma 3.2.** *If  $\mathfrak{M}$  is division then  $|\text{N}(\mathfrak{M})| = n(q^n - 1)$ .*

*Proof.* We define  $\rho : \mathbb{F}_{q^n} \rightarrow \text{End}(\mathbb{F}_{q^n}/\mathbb{F}_q)$  by  $\rho(\xi) : \eta \mapsto \xi\eta$  for all  $\xi, \eta \in \mathbb{F}_{q^n}$ . Since  $\mathfrak{M}$  is division and  $\mathbb{F}_{q^n} \cong \mathbb{F}_{q^n}$  as  $\mathbb{F}_q$ -vector spaces we may assume without loss of generality that  $\mathfrak{M} = \rho(\mathbb{F}_{q^n})$ . Let  $\sigma \in \text{N}(\mathfrak{M})$ . We claim that  $\sigma = \rho(\omega)\varphi$  for a unique  $\omega \in \mathbb{F}_{q^n}$  and  $\varphi \in \text{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ . Set  $\omega := \sigma(1)$  and  $\varphi := \rho(\omega)^{-1}\sigma = \rho(\omega^{-1})\sigma$ . Then  $\varphi(1) = 1$  and  $\varphi^{-1}\mathfrak{M}\varphi = \mathfrak{M}$ , i.e.,  $\varphi \in \text{N}(\mathfrak{M})$ . So, for each  $\xi \in \mathbb{F}_{q^n}$ , there is  $\xi' \in \mathbb{F}_{q^n}$  such that  $\varphi^{-1}\rho(\xi')\varphi = \rho(\xi)$ , i.e.,  $\varphi(\xi\eta) = \xi'\varphi(\eta)$  for all  $\eta \in \mathbb{F}_{q^n}$ . Thus  $\xi' = \varphi(\xi)$  whence  $\varphi(\xi\eta) = \varphi(\xi)\varphi(\eta)$ , i.e.,  $\varphi \in \text{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ , as claimed. Conversely  $\rho(\mathbb{F}_{q^n}^\times)\text{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) \subseteq \text{N}(\mathfrak{M})$ . Since  $|\text{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)| = n$ ,  $|\rho(\mathbb{F}_{q^n}^\times)| = q^n - 1$  and  $\rho(\mathbb{F}_{q^n}^\times) \cap \text{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \{\text{Id}\}$  we are done.  $\square$

**Lemma 3.3.** *If  $\mathfrak{M}$  is split then  $|\text{N}(\mathfrak{M})| = n!(q - 1)^n$ .*

*Proof.* We may assume that  $\mathfrak{M} = \mathfrak{D}$ . It is clear that  $\mathfrak{D}^*\mathfrak{P} \subseteq N(\mathfrak{D})$  where  $\mathfrak{D}^* = \mathfrak{D} \cap \text{GL}(n, q)$  and  $\mathfrak{P}$  is the set of all  $n \times n$  permutation matrices. Conversely let  $U = (\alpha_{i,j}) \in N(\mathfrak{D})$ . If we define  $D_i := \text{diag}(0, \dots, 0, 1, 0, \dots, 0)$  where 1 is in the  $i$ th position then  $D_i U = U D$  for some  $D = \text{diag}(\delta_1, \dots, \delta_n)$ . We have  $(0, \dots, 0, \alpha_{i,j}, 0, \dots, 0)^T = \delta_j(\alpha_{1,j}, \dots, \alpha_{n,j})^T$  by comparing the  $j$ th columns of both sides of  $D_i U = U D$ . Since  $\alpha_{i,j_i} \neq 0$  for some  $j_i$ , we have  $\delta_{j_i} = 1$  so that  $\alpha_{k,j_i} = 0$  for all  $k \neq i$ . Since  $U$  is invertible,  $\alpha_{i,j} = 0$  for all  $j \neq j_i$ . Thus  $U \in \mathfrak{D}^*\mathfrak{P}$ . Since  $|\mathfrak{D}^*| = (q-1)^n$ ,  $|\mathfrak{P}| = n!$  and  $\mathfrak{D}^* \cap \mathfrak{P} = \{I_n\}$  we are done.  $\square$

Recall that there is another expression of a partition  $(n_1, \dots, n_t)$  of  $n$ , i.e.,  $(1^{m_1}, 2^{m_2}, \dots, n^{m_n})$  where  $m_i$  is the multiplicity of  $i$  in  $(n_1, \dots, n_t)$ . For instance we see that  $(4, 2, 2, 1) = (1^1, 2^2, 3^0, 4^1, 5^0, 6^0, 7^0, 8^0, 9^0)$ .

**Lemma 3.4.** *Suppose that  $\mathfrak{M}$  has type  $(1^{m_1}, \dots, n^{m_n})$ . Then*

$$|N(\mathfrak{M})| = \prod_{i=1}^n m_i! (i(q^i - 1))^{m_i}.$$

*Proof.* We may assume that  $\mathfrak{M} = \bigoplus_{i=1}^t \rho_i(\mathbb{F}_i)$  with  $\dim_{\mathbb{K}} \mathbb{F}_i = n_i$  and  $(1^{m_1}, \dots, n^{m_n}) = (n_1, \dots, n_t)$ . By Lemmas 3.2 and 3.3 it is sufficient to prove that if  $U \in N(\mathfrak{M})$  then  $U$  is a block matrix  $(B_{i,j})_{1 \leq i,j \leq t}$  with  $B_{i,j} \in \text{Mat}_{n_i \times n_j}(\mathbb{K})$  such that  $B_{i,j}$  is the zero matrix whenever  $n_i \neq n_j$ . Suppose on the contrary that  $n_i \neq n_j$  and  $B_{i,j} \neq 0$ . Since  $\rho_i(\mathbb{F}_i)B_{i,j} = B_{i,j}\rho_j(\mathbb{F}_j)$  we know from Corollary 2.7 that there exists a nonzero map  $\psi : \mathbb{F}_j \rightarrow \mathbb{F}_i$  such that  $\forall \xi \in \mathbb{F}_j, \exists \xi' \in \mathbb{F}_i, \forall \eta \in \mathbb{F}_j, \psi(\xi\eta) = \xi'\psi(\eta)$ . If we put  $\varphi := \psi(1)^{-1}\psi$  then  $\varphi(1) = 1$  and  $\varphi(\xi\eta) = \xi'\varphi(\eta)$  for all  $\eta \in \mathbb{F}_j$ . Since  $\xi' = \varphi(\xi)$  we have  $\varphi(\xi\eta) = \varphi(\xi)\varphi(\eta)$ , i.e.,  $\varphi$  is a ring homomorphism. So  $\mathbb{F}_i$  becomes an  $\mathbb{F}_j$ -module. It is impossible that  $n_i < n_j$ , because  $\mathbb{F}_j$  itself is an irreducible  $\mathbb{F}_j$ -module. Since  $B_{i,j}^T \rho_i^T(\mathbb{F}_i) = \rho_j^T(\mathbb{F}_j) B_{i,j}^T$  the case  $n_i > n_j$  is impossible, too.  $\square$

**Proposition 3.5.** *We have  $|\text{Cl}(\mathfrak{M})| = |\text{GL}(n, q)| / |N(\mathfrak{M})|$ .*

*Proof.* It follows from the orbit-stabilizer counting principle.  $\square$

Now we recall the important formula of A. Cayley:

**Proposition 3.6.** *For every  $n \in \mathbb{N}$  with indeterminate  $q$  we have*

(i)

$$\sum_{(1^{m_1}, \dots, n^{m_n}) \vdash n} \left( \prod_{i=1}^n \frac{1}{m_i! (i(1 - q^i))^{m_i}} \right) = \prod_{i=1}^n \frac{1}{1 - q^i};$$

(ii)

$$\sum_{(1^{m_1}, \dots, n^{m_n}) \vdash n} \left( \prod_{i=1}^n \frac{1}{m_i! (i(q^i - 1))^{m_i}} \right) = \frac{q^{\frac{n(n-1)}{2}}}{\prod_{i=1}^n (q^i - 1)}.$$

*Proof.* (i) It is the well-known Cayley's formula [1, Example 1, p. 209].  
(ii) Replace  $q$  in (i) by  $1/q$ . And use the fact that  $n = \sum_{i=1}^n im_i$ .  $\square$

**Theorem 3.7.** *The number of all maximal tori in  $\mathfrak{gl}(n, q)$  is  $q^{n(n-1)}$ .*

*Proof.* Recall that  $|\mathrm{GL}(n, q)| = \prod_{i=1}^n (q^n - q^{n-i}) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - 1)$ . So we are done by Proposition 3.6 (ii), because the desired number is

$$\sum_{\mathfrak{M}} |\mathrm{Cl}(\mathfrak{M})| = \sum_{\mathfrak{M}} \frac{|\mathrm{GL}(n, q)|}{|\mathrm{N}(\mathfrak{M})|} = |\mathrm{GL}(n, q)| \times \sum_{\mathfrak{M}} \frac{1}{|\mathrm{N}(\mathfrak{M})|}$$

where the sum is over maximal tori of distinct types.  $\square$

*Remark 3.7.1.* Accidentally, the quantity  $q^{n(n-1)}$  is also well-known as the number of all nilpotent matrices in  $\mathrm{Mat}(n, q)$ . But I do not know whether or not there is a bijection between the set of all maximal tori in  $\mathfrak{gl}(n, q)$  and the set of all nilpotent matrices in  $\mathrm{Mat}(n, q)$ .

#### 4. MAXIMAL TORI IN $\mathfrak{sl}(n, \mathbb{K})$

Throughout this section we also use the symbol  $\mathbb{K}$  as a field of positive characteristic  $p$ . We denote respectively by  $\mathrm{MT}_{\mathfrak{gl}(n, \mathbb{K})}$  and  $\mathrm{MT}_{\mathfrak{sl}(n, \mathbb{K})}$  the sets of all maximal tori in  $\mathfrak{gl}(n, \mathbb{K})$  and  $\mathfrak{sl}(n, \mathbb{K})$ .

We first review very well-known and basic facts in Lie theory. (The proof of Proposition 4.1 (i) comes from [2].)

**Proposition 4.1.** *Suppose  $p > 2$  or  $n > 2$ . Then the following hold:*

- (i) *The only nontrivial ideals of  $\mathfrak{gl}(n, \mathbb{K})$  are  $\mathbb{K}I_n$  and  $\mathfrak{sl}(n, \mathbb{K})$ ;*
- (ii) *If  $p \nmid n$  then there exists no nontrivial ideal of  $\mathfrak{sl}(n, \mathbb{K})$ . If  $p \mid n$  then  $\mathbb{K}I_n$  is the only nontrivial ideal of  $\mathfrak{sl}(n, \mathbb{K})$ .*

*Proof.* (i) Clearly,  $\mathbb{K}I_n$  and  $\mathfrak{sl}(n, \mathbb{K})$  are ideals of  $\mathfrak{gl}(n, \mathbb{K})$ . Suppose that  $\mathfrak{J}$  is a nonzero ideal  $\neq \mathbb{K}I_n$  of  $\mathfrak{gl}(n, \mathbb{K})$ . Let  $X = \sum_{i,j} \alpha_{i,j} E_{i,j} \in \mathfrak{J} \setminus \mathbb{K}I_n$  where  $\alpha_{i,j} \in \mathbb{K}$  and  $E_{i,j}$ 's are elements of the standard basis for  $\mathrm{Mat}(n, \mathbb{K})$ . Assume  $\alpha_{s,t} \neq 0$  for some  $s, t$  with  $s \neq t$ . If  $p > 2$  then  $-2\alpha_{s,t}E_{t,s} = [[X, E_{t,s}], E_{t,s}] \in \mathfrak{J}$ . So  $E_{t,s} \in \mathfrak{J}$ . If  $n > 2$  then choose  $r \neq s, t$ . Then  $\alpha_{s,t}E_{r,s} = [[[X, E_{t,s}], E_{r,s}], E_{r,r}] \in \mathfrak{J}$ . So  $E_{r,s} \in \mathfrak{J}$ . On the other hand, if  $\alpha_{s,t} = 0$  for all  $s, t$  with  $s \neq t$  then  $X = \sum_i \alpha_{i,i} E_{i,i}$  so that  $\alpha_{s,s} \neq \alpha_{t,t}$  for some  $s, t$  with  $s \neq t$ . Since  $(\alpha_{s,s} - \alpha_{t,t})E_{s,t} = [X, E_{s,t}] \in \mathfrak{J}$  we have  $E_{s,t} \in \mathfrak{J}$ . In all cases,  $E_{s,t} \in \mathfrak{J}$  for some  $s, t$  with  $s \neq t$ . Thus,  $E_{i,t} = [E_{i,s}, E_{s,t}] \in \mathfrak{J}$  for all  $i \neq t$ , and  $E_{s,j} = [E_{s,t}, E_{t,j}] \in \mathfrak{J}$  for all  $j \neq s$ . This facts imply that, for all  $i, j$  with  $i \neq j$ ,  $E_{i,j} \in \mathfrak{J}$  and so  $E_{i,i} - E_{j,j} = [E_{i,j}, E_{j,i}] \in \mathfrak{J}$ . Since  $\mathfrak{J}$  is a proper ideal of  $\mathfrak{gl}(n, \mathbb{K})$  we have  $\mathfrak{J} = \mathfrak{sl}(n, \mathbb{K})$ . (ii) Note that  $p \mid n$  if and only if  $I_n \in \mathfrak{sl}(n, \mathbb{K})$ . If  $p \mid n$  then  $\mathbb{K}I_n$  is an ideal of  $\mathfrak{sl}(n, \mathbb{K})$ . Let  $\mathfrak{J}$  be a nonzero ideal  $\neq \mathbb{K}I_n$  of  $\mathfrak{sl}(n, \mathbb{K})$ . The proof is similar with (i) except the case  $n > 2$ , since  $E_{r,r} \notin \mathfrak{sl}(n, \mathbb{K})$ . Thus suppose  $p = 2$  and  $n > 2$ . Then  $\alpha_{s,t}E_{r,s} + \alpha_{s,r}E_{t,s} = [[X, E_{t,s}], E_{r,s}] \in \mathfrak{J}$ . If  $\alpha_{s,r} = 0$  then  $E_{r,s} \in \mathfrak{J}$ . If  $\alpha_{s,r} \neq 0$  then  $\alpha_{s,r}E_{t,s} = [[[X, E_{t,s}], E_{r,s}], E_{r,r} + E_{s,s}] \in \mathfrak{J}$ . So  $E_{t,s} \in \mathfrak{J}$ .  $\square$

*Remark 4.1.1.* Two ideals  $\mathbb{K}I_n$  and  $\mathfrak{sl}(n, \mathbb{K})$  in  $\mathfrak{gl}(n, \mathbb{K})$  are in fact closed under the  $p$ -map, i.e.,  $\mathbb{K}I_n$  and  $\mathfrak{sl}(n, \mathbb{K})$  are *restricted* ideals of  $\mathfrak{gl}(n, \mathbb{K})$ .

Recall that if  $p \nmid n$  then  $\mathfrak{gl}(n, \mathbb{K})$  is a direct sum of two restricted ideals  $\mathbb{K}I_n$  and  $\mathfrak{sl}(n, \mathbb{K})$  in  $\mathfrak{gl}(n, \mathbb{K})$ , that is,  $\mathfrak{gl}(n, \mathbb{K}) = \mathbb{K}I_n \oplus \mathfrak{sl}(n, \mathbb{K})$  as vector spaces and  $[X, Y] = 0$  for every  $X \in \mathbb{K}I_n$  and  $Y \in \mathfrak{sl}(n, \mathbb{K})$ .

**Lemma 4.2.** *Let  $p \nmid n$  and  $\pi : \mathfrak{gl}(n, \mathbb{K}) \rightarrow \mathfrak{gl}(n, \mathbb{K})/\mathbb{K}I_n \cong \mathfrak{sl}(n, \mathbb{K})$  a canonical projection. Then  $\pi$  induces a bijection  $\tilde{\pi} : \text{MT}_{\mathfrak{gl}(n, \mathbb{K})} \rightarrow \text{MT}_{\mathfrak{sl}(n, \mathbb{K})}$  described by  $\tilde{\pi}(\mathfrak{M}) = \mathfrak{M} \cap \mathfrak{sl}(n, \mathbb{K})$  and  $\tilde{\pi}^{-1}(\mathfrak{M}_0) = \mathbb{K}I_n \oplus \mathfrak{M}_0$ .*

*Proof.* If we denote the canonical isomorphism  $\mathfrak{gl}(n, \mathbb{K})/\mathbb{K}I_n \rightarrow \mathfrak{sl}(n, \mathbb{K})$  by  $\varphi$  then it is easy to see that  $\tilde{\pi}(\mathfrak{M}) := (\varphi \circ \pi)(\mathfrak{M}) = \mathfrak{M} \cap \mathfrak{sl}(n, \mathbb{K})$  for each  $\mathfrak{M} \in \text{MT}_{\mathfrak{gl}(n, \mathbb{K})}$ . We know from Proposition 1.1 that, for any  $\mathfrak{M}_0 \in \text{MT}_{\mathfrak{sl}(n, \mathbb{K})}$ , there exists some  $\mathfrak{M} \in \text{MT}_{\mathfrak{gl}(n, \mathbb{K})}$  with  $\mathfrak{M}_0 \subseteq \mathfrak{M}$ . So  $\tilde{\pi}$  is surjective. Since  $p \nmid n$ ,  $I_n \notin \mathfrak{M}_0$  for all  $\mathfrak{M}_0 \in \text{MT}_{\mathfrak{sl}(n, \mathbb{K})}$ . Since  $I_n \in \mathfrak{M}$  for each  $\mathfrak{M} \in \text{MT}_{\mathfrak{gl}(n, \mathbb{K})}$  by Proposition 2.1 (ii),  $\tilde{\pi}$  is injective.  $\square$

**Lemma 4.3.** *Suppose  $p > 2$  or  $n > 2$ . If  $p \mid n$  and we define  $\psi : \text{MT}_{\mathfrak{gl}(n, \mathbb{K})} \rightarrow \text{MT}_{\mathfrak{sl}(n, \mathbb{K})}$  by  $\mathfrak{M} \mapsto \mathfrak{M} \cap \mathfrak{sl}(n, \mathbb{K})$  then  $\psi$  is a bijection.*

*Proof.* We define  $\eta : \text{MT}_{\mathfrak{sl}(n, \mathbb{K})} \rightarrow \text{MT}_{\mathfrak{gl}(n, \mathbb{K})}$  by  $\eta(\mathfrak{M}_0) := \langle \mathfrak{M}_0 \rangle$  where  $\langle \mathfrak{M}_0 \rangle$  is the associative  $\mathbb{K}$ -algebra in  $\text{Mat}(n, \mathbb{K})$  generated by  $\mathfrak{M}_0$ . If we prove  $\eta$  to be well-defined then the proof will be done, because  $\eta$  is obviously the inverse of  $\psi$ . So we claim  $\dim \langle \mathfrak{M}_0 \rangle = n$ . Assume to the contrary that  $\langle \mathfrak{M}_0 \rangle = \mathfrak{M}_0$ . Then  $\mathfrak{M}_0 = \bigoplus_{i=1}^s \mathbb{E}_i$  for some separable extension fields  $\mathbb{E}_1, \dots, \mathbb{E}_s$  of  $\mathbb{K}$  as in the proof of Corollary 2.3. We put  $r_i := \text{rank}(1_{\mathbb{E}_i})$ ,  $d_i := [\mathbb{E}_i : \mathbb{K}]$  and  $m_i := r_i/d_i$  for each  $i \in \{1, \dots, s\}$ . Note that  $m_i$ 's are integers and, for all  $X = \sum_i X_i \in \mathfrak{M}_0$  with  $X_i \in \mathbb{E}_i$ ,

$$\text{Tr}(X) = \sum_{i=1}^s m_i \text{Tr}_{\mathbb{E}_i/\mathbb{K}}(X_i).$$

Since  $\sum_i d_i = n - 1$  and  $\sum_i m_i d_i = \sum_i r_i = n$  we can see that  $m_j = 2$  and  $d_j = 1$  for some  $j \in \{1, \dots, s\}$ , and  $m_i = 1$  for each  $i \neq j$ . Suppose  $p > 2$ . Since  $p \nmid m_j = 2$ ,  $m_j \text{Tr}_{\mathbb{E}_j/\mathbb{K}}$  is not identically zero. So  $\text{Tr}(\mathfrak{M}) \neq 0$ , a contradiction. Suppose  $n > 2$ . Then  $s \geq 2$ . Since  $m_i = 1$  for  $i \neq j$ ,  $m_i \text{Tr}_{\mathbb{E}_i/\mathbb{K}}$  is not identically zero. So  $\text{Tr}(\mathfrak{M}) \neq 0$ , a contradiction.  $\square$

*Remark 4.3.1.* Suppose  $p = n = 2$ . Then the unique maximal torus in  $\mathfrak{sl}(2, \mathbb{K})$  is  $\mathbb{K}I_2$ . Therefore the map  $\psi$  is clearly not injective.

**Corollary 4.4.** *Suppose  $p > 2$  or  $n > 2$ . For each  $q = p^\ell$  with  $\ell \in \mathbb{N}^+$ , the number of all maximal tori in  $\mathfrak{sl}(n, q)$  is  $q^{n(n-1)}$ .*

*Proof.* This result is due to Lemmas 4.2, 4.3 and Theorem 3.7.  $\square$

**Corollary 4.5.** *Suppose  $p > 2$  or  $n > 2$ . Then every maximal torus in  $\mathfrak{sl}(n, \mathbb{K})$  is self-centralizing.*

*Proof.* Let  $\mathfrak{M}_0 \in \text{MT}_{\mathfrak{sl}(n, \mathbb{K})}$  and assume that  $\mathfrak{M}_0 \subsetneq C_{\mathfrak{sl}(n, \mathbb{K})}(\mathfrak{M}_0)$ . Choose  $X \in C_{\mathfrak{sl}(n, \mathbb{K})}(\mathfrak{M}_0) \setminus \mathfrak{M}_0$ . We consider two cases: (a)  $p \nmid n$  and (b)  $p \mid n$ . (a) If  $p \nmid n$  then  $X$  centralizes  $\mathfrak{M} := \mathbb{K}I_n \oplus \mathfrak{M}_0$  which is in  $\text{MT}_{\mathfrak{gl}(n, \mathbb{K})}$  by Lemma 4.2. (b) If  $p \mid n$  then  $X$  centralizes  $\mathfrak{M} := \langle \mathfrak{M}_0 \rangle$  which is in  $\text{MT}_{\mathfrak{gl}(n, \mathbb{K})}$  by Lemma 4.3. In any case,  $X \in \mathfrak{M}$  by Proposition 1.3. Since  $X \in \mathfrak{sl}(n, \mathbb{K})$  we have  $X \in \mathfrak{M} \cap \mathfrak{sl}(n, \mathbb{K}) = \mathfrak{M}_0$ , a contradiction.  $\square$

#### REFERENCES

- [1] G. E. Andrews, The theory of partitions, *Cambridge University Press*, Cambridge, 1998 (Reprint of the 1976 original).
- [2] N. Jacobson, Abstract derivation and Lie algebras, *Trans. Amer. Math. Soc.* 42 (1937), no. 2, 206-224.
- [3] D. Winter, On the toral structure of Lie  $p$ -algebras, *Acta Math.* 123 (1969), 69-81.

DEPARTMENT OF MATHEMATICS, PUSAN NATIONAL UNIVERSITY, JANG-JEON DONG, BUSAN, REPUBLIC OF KOREA

*E-mail address:* poissonn00@hanmail.net